認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正

評価対象

申請受付日（受付番号）	平成26年3月24日 (IT認証4497)
認証番号	C0450
認証申請者	シャープ株式会社
TOEの名称	MX-FR44
TOEのバージョン	C.10
PP適合	なし
適合する保証パッケージ	EAL3
開発者	シャープ株式会社
評価機関の名称	一般社団法人　ITセキュリティセンター　評価部

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。

平成26年11月27日

技術本部
セキュリティセンター 情報セキュリティ認証室
技術管理者　山里　拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 リリース4

② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース4

評価結果：合格

「MX-FR44 C.10」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、シャープ株式会社が開発した「MX-FR44 C.10」（以下「TOE」という。）について一般社団法人　ITセキュリティセンター　評価部（以下「評価機関」という。）が平成26年11月に完了したITセキュリティ評価に対し、その内容の認証結果を申請者であるシャープ株式会社に報告するとともに、TOEに関心を持つ消費者や調達者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書の付属書であるセキュリティターゲット（以下「ST」という。）を併読されたい。特にTOEのセキュリティ機能要件、保証要件及びその十分性の根拠は、STにおいて詳述されている。

本認証報告書は、市販されるTOEを購入する一般消費者、及び調達者を読者と想定している。本認証報告書は、TOEが適合する保証要件に基づいた認証結果を示すものであり、個別のIT製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

TOEの機能、運用条件の概要を以下に示す。詳細は2章以降を参照のこと。

1.1.1 保証パッケージ

TOEの保証パッケージは、EAL3である。

1.1.2 TOEとセキュリティ機能性

TOEはデジタル複合機（以下「MFD」という。）内データ保護機能を持つIT製品である。

TOEの主要部分は、ROM及びHDDに格納されたMFD用ファームウェアである。これはMFDの標準ファームウェアを置き換えることにより、セキュリティ機能を提供すると共にMFD全体の制御を行う。MFD内蔵ハードウェアの一部であるHDCがTOEに含まれ、ファームウェア部分から呼び出される。

TOEの主要なセキュリティ機能は、暗号操作機能、データ消去機能、親展ファイル機能、ネットワーク保護機能、ファクスフロー制御機能であり、TOEを搭載したMFD内部のイメージデータを不正に取得する試みに対抗することを目的とする。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。TOEが想定する脅威及び前提につ

いては次項のとおり。

1.1.2.1 脅威とセキュリティ対策方針

TOEは以下の脅威を想定しており、それに対抗するセキュリティ機能を提供する。

TOEの保護資産である、MFD内に保存されたイメージデータ、アドレス帳データ等の利用者データは、TOEの不正操作、記憶媒体からの直接的な読み取り、ネットワーク経路上の通信データへのアクセス等により、不正に暴露されたり改ざんされたりする脅威が想定される。

この脅威に対抗するため、MFD内部のHDD（以下「MSD」という。）への書き込み時に暗号化することにより直接情報を読み取られることを防ぐ。また、イメージデータを保存する際にパスワードによる保護機能を提供し、許可されない利用者がデータにアクセスすることを防ぐ。さらにネットワーク通信において暗号化による保護機能を提供し、通信データが盗聴されることを防ぐ。

セキュリティ機能の設定内容については、管理者の識別認証を行い、不正に設定変更やセキュリティ機能を無効化されることを防ぐ。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定している。

TOEは、シャープ株式会社が提供するMFD上で動作する。

TOEが搭載されたMFDは、内部ネットワークにクライアント、各種サーバーと共に接続され利用される事を想定している。

内部ネットワークが外部ネットワークと接続する場合は、外部ネットワークからMFDに対するアクセスを遮断するためファイアウォールが接続される。

1.1.3 免責事項

TOE、クライアント間の通信を保護するためのセキュリティ機能が動作しない環境においては、運用者の責任で通信保護のための対策を行う必要がある。詳細は4.3章を参照のこと。

1.2 評価の実施

認証機関が運営するITセキュリティ評価・認証制度に基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[1]、「ITセキュリティ認証等に関する要求事項」[2]、「ITセキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によってTOEに関わる機能要件及び保証要件に基づいてITセキュリティ評価が実施され、平成26年11月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、その他関連する評価証拠資料を検証し、TOEの評価が所定の手続きに沿って行われたことを確認した。その結果、TOEの評価がCC（[4][5][6]または[7][8][9]）及びCEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は本認証報告書を作成し、認証作業を終了した。

2 TOE識別

TOEは、以下のとおり識別される。

TOE名称：	MX-FR44
バージョン：	C.10
開発者：	シャープ株式会社

上記TOE名称は、シャープ社製MFDのセキュリティ機能を強化するためのオプション製品を示す。

製品が評価･認証を受けたTOEであることを、利用者は以下の方法によって確認することができる。

TOE添付のガイダンス文書に記載された手順に従い、操作パネル上にTOEの名称及びバージョンを表示し、その内容とガイダンス文書に記載された名称、バージョンを比較する事により、利用者は設置された製品が評価を受けたTOEであることを確認できる。

3　セキュリティ方針

本章では、TOEがセキュリティサービスとしてどのような方針あるいは規則のもと、機能を実現しているかを述べる。

TOEはMFD内部のイメージデータに対する不正なアクセスに対抗するためのセキュリティ機能、及びネットワーク上の通信データを保護するためのセキュリティ機能を提供する。

TOEは組織のセキュリティ方針を満たすため、内部の保存データを上書き消去する機能、ファクスI/Fを経由した電話回線網からの不正アクセスを防ぐ機能を提供する。

また、上記セキュリティ機能に関する各種設定を管理者のみが行えるよう制限することで、セキュリティ機能の無効化や不正使用を防止する。

3.1　セキュリティ機能方針

TOEは、3.1.1に示す脅威に対抗し、3.1.2に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1　脅威とセキュリティ機能方針

3.1.1.1　脅威

TOEは、表3-1に示す脅威を想定し、これに対抗する機能を備える。

表3-1　想定する脅威

識別子	脅　威
T.RECOVER	攻撃者が、MFDからMSDを取り外して持ち出し、他の装置（そのMSDを搭載したMFD以外の装置）を接続することにより、MSD内の利用者データを読み出し漏えいさせる。
T.REMOTE	MFDへのアクセスを認められていない攻撃者が、内部ネットワーク経由でMFD内のアドレス帳データを、まとめて読み出しまたは改変する。
T.SPOOF	攻撃者が、他の利用者になりすますことにより、操作パネルまたは内部ネットワーク経由で、利用者が親展ファイルとしてファイリング保存したイメージデータを、読み出し漏えいさせる。
T.TAMPER	攻撃者が、管理者になりすますことにより、操作パネルまたは内部ネットワーク経由で、ネットワーク設定データを、読み出しまたは改変する。

T.TAP	正当な利用者がMFDに対して通信する際、攻撃者が内部ネットワーク上の通信データを盗聴する。

3.1.1.2 脅威に対するセキュリティ機能方針

TOEは、表3-1に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

(1) 脅威「T.RECOVER」への対抗

本脅威はMFDから取り外されたMSDから、内部に残存するデータが漏えいすることを想定している。この脅威に対して下記のセキュリティ機能により対抗する。

① 暗号鍵生成機能（TSF_FKG）

暗号鍵（共通鍵）の生成を行い、暗号操作機能（TSF_FDE）をサポートする機能である。TOEは、MFDの電源がオンになると必ず256ビット長のセキュアな暗号鍵（共通鍵）を生成し、揮発性メモリー内に保存する。

② 暗号操作機能（TSF_FDE）

利用者データ及びTSFデータをMSDに書き込む必要が生じたときは、必ずそれらのデータを暗号化してから書き込む。また、それらのデータが必要になれば、MSDから読み出し、復号して利用する。暗号化及び復号にはFIPS PUB 197に基づくAESアルゴリズム、及び暗号鍵生成機能（TSF_FKG）により生成された暗号鍵を用いる。

対象となる利用者データは、HDD上のスプールイメージデータ、HDD上のファイリングイメージデータ、HDD上のアドレス帳データである。また、対象となるTSFデータは、HDD上の親展ファイルパスワード、HDD上の管理者パスワードである。

(2) 脅威「T.REMOTE」、「T.TAP」への対抗

本脅威はTOEが管理するアドレス帳データに対して内部ネットワーク経由で不正なアクセスが行われること、及びクライアントとの通信データが盗聴により漏えいすることを想定している。この脅威に対して下記のセキュリティ機能により対抗する。

① ネットワーク保護機能（TSF_FNP）

ネットワーク保護に関する以下の3機能を提供する。

a）フィルタ機能

管理者による事前の設定に基づき、意図しない通信相手との通信を拒絶する。IPアドレスによる条件とMACアドレスによる条件を設定できる。

条件に合わない通信相手からのネットワークパケットを、必ず破棄し、レスポンス及び処理をしない。

IPアドレスによる条件は、範囲を四つまで指定し、それらを許可するかまたは拒否するかを指定する。MACアドレスによる条件は、許可するMACアドレスを10個まで指定する

b) 通信データ保護機能

次の通信データ保護機能を提供する。

- クライアントとTOEのWebとの通信を、盗聴より保護できるよう、HTTPS通信機能を提供する。
- クライアントのプリンタードライバーから送信される印刷データを、盗聴より保護できるよう、IPP-SSL通信機能を提供する。

上記設定の問い合わせ及び改変を、認証機能(TSF_AUT)で識別認証された管理者のみに許す。また、各通信の使用/未使用（無効）の設定によって、ネットワーク保護機能の動作を変更することができる。

c) ネットワーク設定保護機能

ネットワーク設定データを扱うインタフェースを、操作パネル及びTOEのWebで提供する。これらのインタフェースは管理者のみに対して提供し、他の利用者のアクセスより保護する。

(3) 脅威「T.TAMPER」への対抗

本脅威はTOEが管理するネットワーク設定データに対して、操作パネルまたは内部ネットワーク経由で不正なアクセスが行われることを想定している。この脅威に対しては下記のセキュリティ機能により対抗する。また、クライアントからの通信データについてはネットワーク保護機能（TSF_FNP）の通信データ保護機能により保護される。

① 認証機能（TSF_AUT）

管理者パスワードにより管理者の識別認証を行う。長さ5文字以上のパスワードのみを受け入れる。正しい管理者パスワードによって管理者認証に成功した場合に限り、管理者向け機能へのインタフェースを提供する。操作パネルでの管理者パスワード入力時、入力した文字と同数のアスタリスク（星型記号）を表示するが、入力した文字は表示しない。Webブラウザーからの管理者パスワード入力時は、入力された文字を代替文字のような方式で隠蔽するようWebブラウザーに対して要求する。

管理者パスワード認証において、連続して3回認証に失敗した場合、認証受付を停止、すなわち管理者パスワードをロックする。ロックからの経

過時間が5分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアしてロック状態から復帰する。

管理者のみに管理者パスワードの変更（改変）機能を提供することにより、役割の維持管理を図る。

(4) 脅威「T.SPOOF」への対抗

本脅威はTOEに親展ファイルとしてファイリング保存されたイメージデータに対して、操作パネルまたは内部ネットワーク経由で不正なアクセスが行われることを想定している。この脅威に対しては下記のセキュリティ機能（親展ファイル機能）により、正当な親展ファイル保存者を識別認証することで対抗する。また、識別認証に使用される親展ファイルパスワードについては、ネットワーク保護機能（TSF_FNP）の通信データ保護機能、及び暗号操作機能（TSF_FDE）により保護される。

① 親展ファイル機能（TSF_FCF）

MFD内に利用者が親展ファイルとして保存したイメージデータをパスワード保護し、操作パネルまたはWeb経由での認証を経て再操作（印刷等）を許す機能を提供する。

親展ファイルの再操作に先立つ親展ファイルパスワード認証では、入力文字を隠蔽し、連続して3回認証に失敗した場合、当該親展ファイルをロックする。失敗回数は、各ファイルについて数える。認証に成功したとき、当該ファイルの失敗回数をゼロに戻す。ロックの解除は、認証(TSF_AUT)で識別認証された管理者のみに許される。

再操作の一種として親展ファイルパスワード変更の機能を、本TSFで識別認証された親展ファイル保存者のみに提供し、新パスワードが5文字以上であることを検査する。

なお、以下のとおりドキュメントファイリング機能に関する管理機能を持ち、認証(TSF_AUT)で識別認証された管理者に実行を許す。

a）親展ファイルによる保護の実効性を高めるための管理機能

- ドキュメントファイリング禁止設定
  ジョブ種類別に各保存モードを禁止できる。親展でない（パスワードのない）モードをすべて禁止する設定が既定値であり、推奨値である。

- ホールド以外のプリントジョブ制限設定
  プリンタードライバーからのジョブに対し、その場での印刷出力を制限する。ホールド指定のないジョブは拒否または強制的にホールドし、ホールドするジョブは印刷の有無を無視してホールドのみ行う。出力

された用紙が第三者に持ち去られるリスクの高い環境において推奨される。

b) 親展ファイルのロックに関する管理機能

- 親展ファイルのロック解除
  親展ファイルパスワード認証失敗によりロックされた親展ファイルに対し、ロックを解除する。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表 3-2に示す。

表 3-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
P.RESIDUAL	ジョブ完了または中止時、MSDにスプール保存された利用者データの領域は、少なくとも1回上書き消去されなければならない。 MSDにおいて、利用者が削除した利用者データの領域は、少なくとも1回上書き消去されなければならない。 MFDの廃棄または所有者変更の際、MSDの利用者データの領域はすべて、少なくとも1回上書き消去されなければならない。
P.FAXTONET	MFDのファクスI/Fに接続される電話回線網からは、MFDのネットワークI/Fを経由しての内部ネットワークへのアクセスを、できないようにしなければならない。

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOEは、表 3-2に示す組織のセキュリティ方針を下記のセキュリティ機能により満たす。

(1) 組織のセキュリティ方針「P.RESIDUAL」の実現

「P.RESIDUAL」はMSDに保存される利用者データ領域に対して上書き消去を求めている。この組織のセキュリティ方針を下記のセキュリティ機能により実現する。

① データ消去機能（TSF_FDC）

HDDに保存された利用者データ、すなわち、スプール保存及びファイリング保存されたイメージデータファイル、またはアドレス帳ファイルを消去する機能を提供する。本機能は、以下の各機能により構成される。各機能ともHDDにランダム値を上書きすることにより、イメージデータの再生を不能とする。

a) 各ジョブ完了後の自動消去
下記機能により構成される。

- ジョブ処理のためHDDにスプール保存されたイメージデータを、当該ジョブ完了または中止時に上書き消去する機能
- ドキュメントファイリング機能（親展ファイル機能を含む）によりHDDに保存されたイメージデータを、利用者の操作により削除される際に上書き消去する機能

b) 全データエリア消去
認証機能（TSF_AUT）で識別認証された管理者により操作パネルにて起動され、HDDにスプール保存及びファイリング保存された全てのイメージデータを上書き消去する機能である。

本機能は途中での中止機能を提供する。キャンセル操作が選択されると、管理者の識別認証を必ず要求し、正しく識別認証された場合についてのみ上書き消去を中止する。認証入力中、入力した文字と同数のアスタリスク（星型記号）を表示するが、入力した文字は表示しない。また、認証入力中、連続して3回認証に失敗した場合、認証受付を停止、すなわち管理者パスワードをロックする。ロックからの経過時間が5分に達すれば、自動的にロックを解除、すなわち、認証失敗回数をクリアしてロック状態から復帰する。

c) アドレス帳/本体内登録データ消去
認証機能（TSF_AUT）で識別認証された管理者の操作により、HDD上のアドレス帳データを上書き消去する機能である。

d) ドキュメントファイリングデータ消去
認証機能（TSF_AUT）で識別認証された管理者の操作により、HDD上のイメージデータを上書き消去する機能である。対象データは以下の選択肢から一つ以上を、起動時に管理者が指定する。

- HDD上にあるすべてのスプールイメージデータ
- HDD上にあるすべてのファイリングイメージデータ

また本機能は、全データエリア消去と同様の中止機能を持つ。

(2) 組織のセキュリティ方針「P.FAXTONET」の実現

「P.FAXTONET」は、MFDのファクスI/Fで接続された電話回線網から、MFDのネットワークI/F経由での内部ネットワークへのアクセス防止を求めている。この組織のセキュリティ方針を下記のセキュリティ機能により実現する。

① ファクスフロー制御機能（TSF_FFL）

ファクス回線からの通信データに対し、内部ネットワークへ中継することを決して許可しないようなフロー制御を実施する。これにより、MFDのファクスI/Fに接続される電話回線網からの、MFDのネットワークI/Fを経由しての内部ネットワークへのアクセスを防ぐ。

4 前提条件と範囲の明確化

本章では、想定する読者がTOEの利用の判断に有用な情報として、TOEを運用するための前提条件及び使用環境について記述する。

4.1 使用及び環境に関する前提条件

TOEを運用する際の前提条件を表4-1に示す。

これらの前提条件が満たされない場合、TOEのセキュリティ機能が有効に動作することは保証されない。

表 4-1 前提条件

識別子	前提条件
A.NETWORK	TOEを搭載するMFDは、外部ネットワークからの攻撃から保護された内部ネットワークにおける、MFDとの通信を認める機器だけが接続されたサブネットワークに接続するものとする。
A.OPERATOR	管理者は、TOEに対して不正をせず信頼できるものとする。

4.2 使用環境と構成

TOEはシャープ株式会社が提供するMFD上で動作する。対象となる機種はMX-M365FN, MX-M365N, MX-M365NJ, MX-M465FN, MX-M465N, MX-M465NJ, MX-M565FN, MX-M565N,及びMX-M565NJである。

またTOEが搭載されたMFDは内部ネットワークにクライアントPC、各種サーバーと共に接続され利用されることを想定している。また、FAX通信に使用するため電話回線網に接続される。

TOEを設置するMFDの利用環境を図 4-1に示す。
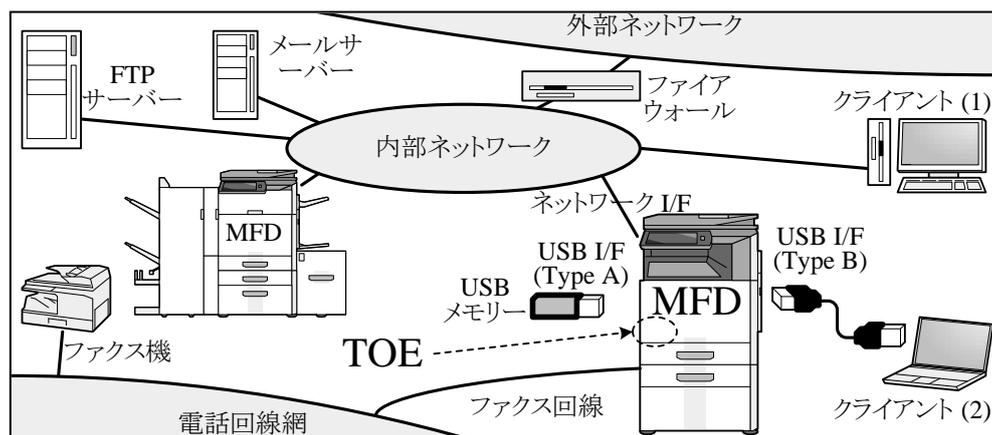
図 4-1 TOEの使用環境

図 4-1に示すように、TOEが搭載されたMFDは内部ネットワーク、及び電話回線網に接続される。内部ネットワークにはクライアントや必要に応じてFTPサーバー、メールサーバー等のサーバーが接続され、TOEと印刷データ等の通信を行う。

内部ネットワークが外部ネットワークと接続する場合は、ファイアウォールを介して接続され、外部ネットワークからMFDに対するアクセスを遮断するための適切な設定が行われる。

4.3 使用環境におけるTOE範囲

TOEは、クライアントとの通信データを保護するためのセキュリティ機能（通信データ保護機能）を提供する。この機能が管理者により未使用（無効）の設定で運用される環境、もしくはこの機能に未対応のクライアントがTOEに接続される環境においては、クライアントとの通信データを保護するための対策（暗号化装置の導入等）を講じる必要があり、それらは運用者の責任となる。

5　アーキテクチャに関する情報

本章では、TOEの物理的な範囲と論理的構成について、目的と関連を説明する。

5.1　TOE境界と論理的構成

TOEの物理的範囲を図 5-1に網掛けで示す。TOEの主要部分はMFDのコントローラーファームウェアである。これはROM及びUSBメモリーにて、シャープ製MFDのセキュリティを強化するためのオプション製品“データセキュリティキット MX-FR44”（DSK）として提供される。セキュリティ機能の一部をMFDのHDC内に実装しており、これもTOEの範囲に含む。

- ROM
  コントローラーファームウェアの一部を格納する。MFDにTOEを設置する際、コントローラー基板に取り付ける。
- MAIN
  コントローラーファームウェアの一部。DSKのUSBメモリーからMFD内のHDDに設置する。
- HDC
  コントローラー基板上の集積回路部品の一部として予めMFDに内蔵されている。
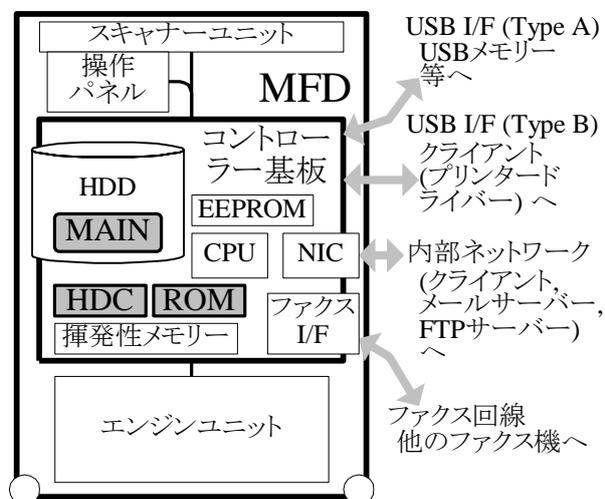
図 5-1　TOE境界

TOEの論理的構成を図 5-2に示す。TOEの論理的範囲を太い枠線内として示す。TOE外のハードウェアを、角を丸くした長方形で示す。TOEの機能を長方形で示し、その中のセキュリティ機能を網掛けで示す。また、揮発性メモリー、HDD、及びEEPROM上にあるデータのうち、セキュリティ機能が扱うデータ（利用者データ及びTSFデータ）を、同じく網掛けで示す。図中、データの流れを矢印で示す。
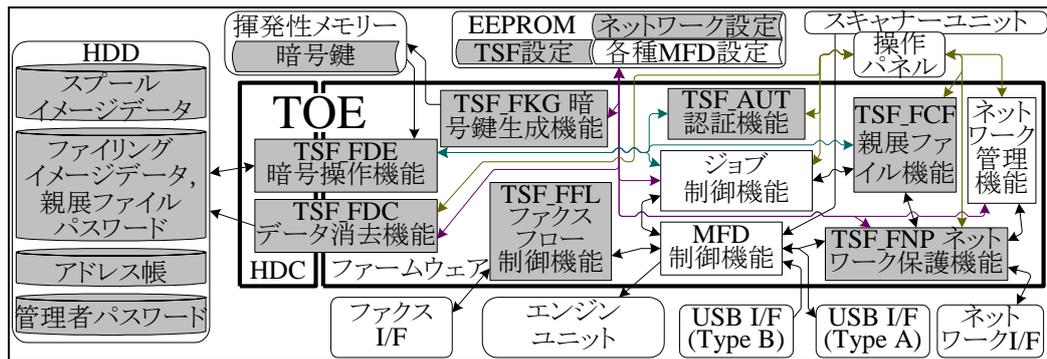
図 5-2　TOE論理構成

TOEの主要部分は、MFD用のファームウェアであり、セキュリティ機能を提供すると共に、MFD全体の制御を行う。また、TOEセキュリティ機能（TSF）の一部はHDC内に実装され、ファームウェア内のTSFから呼び出される。以下がセキュリティ機能である。

a) 暗号操作機能

MSDに書き込む利用者データ、及びTSFデータを暗号化する。また、MSDから読み出した利用者データ、及びTSFデータを復号する。

b) 暗号鍵生成機能

暗号操作機能で使用する暗号鍵を生成する。

c) データ消去機能

HDDからの情報漏洩を防ぐため、HDDに対し上書き消去する。

d) 認証機能

管理者パスワードにより管理者の識別認証を行う。管理者パスワードを変更する管理機能を持つ。

e) 親展ファイル機能

利用者がMFD内にイメージデータを保存する際、他人が無断で再利用しないよう、パスワードによる保護機能を提供する。

f) ネットワーク保護機能

ネットワーク経由の不正アクセス、通信データの盗聴、及び、ネットワーク設定の不正な改変を防ぐ。

g) ファクスフロー制御機能

MFDのファクスI/Fに接続される電話回線網から、MFDのネットワークI/Fを経由して内部ネットワークにアクセスすることを防ぐ。

5.2 IT環境

TOEは内部ネットワークに接続され、FTPサーバー、メールサーバー等のサーバー、及びクライアントと通信を行う。またUSB接続されたクライアント、ファクス回線で接続されたファクス機とも通信を行う。

内部ネットワーク及びUSB経由で接続されたクライアントは、プリンタードライバーやWebブラウザーを介してTOEを利用する。クライアントはWebブラウザーを介してセキュリティ機能に関する設定等の操作を行う事ができる。

6 製品添付ドキュメント

TOEに添付されるドキュメントの識別を以下に示す。TOEの利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。[ ]には各文書のバージョンを示す。

・【日本向け】取扱説明書 データセキュリティキット MX-FR44 [1.0]
・【日本以外向け】MX-FR44 Data Security Kit Operation Guide [1.0]

TOEの取扱説明書として提供され、セキュリティ機能の使い方、設定方法等TOEの管理、運用に必要な事項が記載される。

・【日本向け】注意書 データセキュリティキット MX-FR44 [1.0]
・【日本以外向け】MX-FR44 Data Security Kit Notice [1.0]

TOEをセキュアに利用するための注意事項、及びTOEを複合機本体に取り付ける際の作業手順等が記載される。

7　評価機関による評価実施及び結果

7.1　評価機関

評価を実施した一般社団法人ITセキュリティセンター 評価部は、ITセキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）と相互承認している認定機関（独立行政法人評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2　評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

7.3　評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成26年3月に始まり、平成26年11月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成26年5月、8月に開発現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付・開発セキュリティの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成26年8月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

7.4 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.4.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価した開発者テストの概要を以下に示す。

1) 開発者テスト環境

開発者が実施したテストの構成を図 7-1、表 7-1に示す。
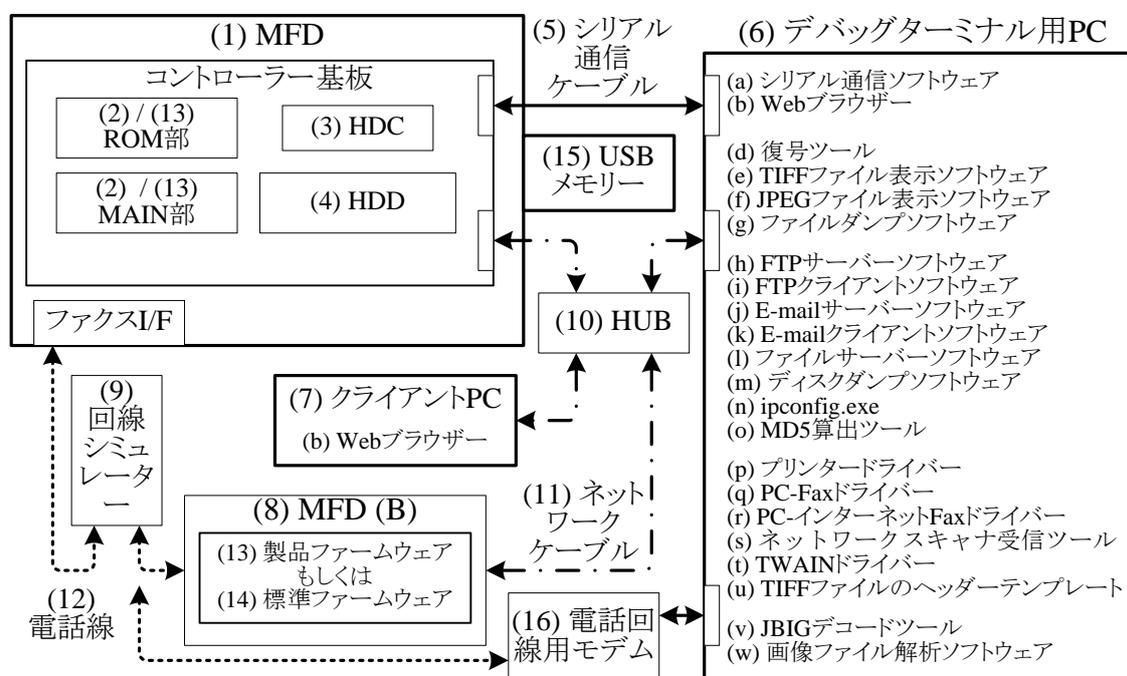
図 7-1 開発者テストの構成図

表 7-1 主な構成要素

構成要素の名称	概要（使用目的）
MFD	TOEが搭載されるMFD。
デバッグターミナル用PC	テストで使用される各種ソフトウェアがインストールされたコンピューター。
クライアントPC	フィルタ機能のテストで使用するためのコンピューター。

回線シミュレータ	ファクス回線（公衆回線）をシミュレートするための機器。
MFD（B）	ファクスや連結印刷等、2台のMFDが必要となるテストで使用する。
電話回線用モデム	公衆回線を通じてデータ通信を行うための機器。

テストで使用されたMFDはSTで識別されている複数のMFDの一部の機種(MX-365FN)が使用された。TOEの動作する各MFDは処理能力等が異なるが、TOEは全て同一なものが使用される。よって、テスト環境は、STにおいて識別された環境と同等の構成であるとみなすことができる。

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

＜開発者テスト手法＞

図7-1に示した環境下で、製品ファームウェア、テスト用ファームウェアの2種類のファームウェアをテストの特性により使い分けて実施した。テスト用ファームウェアは、テストの結果確認のためにシリアルポート出力、暗号鍵の種及び暗号鍵の出力、暗号操作の有効無効の切り替え、上書き消去データの指定を可能にしたものであり、テスト対象のセキュリティ機能性には影響がない。

テスト手法は、インタフェースを刺激する手法(MFDの電源操作、MFDの操作パネルからの手動操作、クライアントPCからの手動操作等)と、応答を観察する手法(MFDの操作パネルからの観察、デバッグターミナルからの観察等)により実施した。

＜開発者テストツール＞

開発者テストにおいて利用したツールを表7-2に示す。

表 7-2　開発者テストツール

	ソフトウェア種別	概要
(a)	シリアル通信ソフトウェア	MFDをシリアル通信を介して操作するためのターミナルエミュレータソフトウェア。
(b)	Webブラウザー	MFDのWebサーバーにアクセスし、MFDを操作、及びMFDの機能であるWebプリント機能（プリント機能）により印刷データをMFDに送信するためのHTTPクライアントソフトウェア。
(d)	復号ツール	MFDで暗号化し作成されたデータファイルを任意の鍵で復号するためのソフトウェア。
(e)	TIFFファイル表示ソフトウェア	MFDで生成される圧縮画像（JBIG、MMR）をPC上で表示するための画像表示ソフトウェア。
(f)	JPEGファイル表示ソフトウェア	MFDで生成される圧縮画像（JPEG）をPC上で表示するための画像表示ソフトウェア。
(g)	ファイルダンプソフトウェア	PC上のファイルを16進数で見ることのできるソフトウェアで、一般的にバイナリエディタと呼ばれるもの。
(h)	FTPサーバーソフトウェア	ネットワークを介し、MFDの機能であるScan-To-FTP機能（スキャン送信機能）を実施、及びデバッグ用のデータをMFDから転送するためのFTPサーバーソフトウェア。
(i)	FTPクライアントソフトウェア	MFDの機能であるScan-To-FTP機能（スキャン送信機能）によりFTPサーバーに転送されたデータを受信、及びFTP Pushプリント機能（プリント機能）により印刷データをMFDに送信するためのFTPクライアントソフトウェア。
(j)	E-mailサーバーソフトウェア	MFDの機能であるScan-To-Email機能、及びインターネットFax機能（いずれもスキャン送信機能）を実施するためのE-mailサーバーソフトウェア。
(k)	E-mailクライアントソフトウェア	MFDの機能であるScan-To-Email機能（スキャン送信機能）によりメールサーバーに転送されたデータを受信、及びE-mailプリント機能（プリント機能） により印刷データをMFDに送信するためのE-mailクライアントソフトウェア。
(l)	ファイルサーバーソフトウェア	MFDの機能であるScan-To-SMB機能（スキャン送信機能）を実施するためのファイルサーバーソフトウェア。
(m)	ディスクダンプソフトウェア	HDD内の任意のセクタを読み込み、その内容を表示、編集できるソフトウェア。
(n)	ipconfig.exe	コマンドプロンプトにおいて、クライアントPCのネットワークインタフェースに設定されているIPアドレス、MACアドレスなどを問い合わせ、改変するためのソフトウェア。
(o)	MD5算出ソフトウェア	コマンドプロンプトにおいて、ファイルまたは文字列に対するMD5値を求めるためのソフトウェア。
(p)	プリンタードライバー	クライアントPCのアプリケーションからMFDで印刷を行うためのプリンタードライバーソフトウエア。
(q)	PC-Faxドライバー	クライアントPCのアプリケーションからMFDでPC-Faxを行うためのPC-Faxドライバーソフトウェア。
(r)	PC-インターネットFaxドライバー	クライアントPCのアプリケーションからMFDでPC-インターネットFaxを行うためのPC-インターネットFaxドライバーソフトウェア。

	ソフトウェア種別	概要
(s)	ネットワークスキャナ受信ツール	MFDの機能であるScan-To-DeskTop機能(スキャン送信機能)によりクライアントPCに転送されたデータを受信するためのクライアントソフトウェア。
(t)	TWAINドライバー	MFDの機能であるリモートPCスキャン機能(スキャン送信機能)を実施するためのTWAINドライバーソフトウェア。
(u)	TIFFファイルのヘッダテンプレート	テストで使用するイメージデータ変換用のTIFFファイルヘッダ。
(v)	JBIGデコードツール	MFDで生成された圧縮画像ファイルをデバッグツール上で表示するための画像データ変換ソフトウェア。
(w)	画像ファイル解析ソフトウェア	MFDで生成されたバイナリファイルをデバッグターミナル用PC上に展開して表示をおこなうことが出来るようにするためのソフトウェア。

＜開発者テストの実施＞

インタフェースの刺激手法としては、MFDの電源操作、MFDの操作パネルの手動操作、クライアントPCからWebブラウザー等を経由した手動操作、他MFDからのネットワークケーブルを経由したデータ送信、回線シミュレータを使用したダイアルアップ接続操作が行われている。

応答の確認手段としては、クライアントPCのWebブラウザーや操作画面に表示された振る舞いの結果観察、MFD操作パネルに表示された振る舞いの結果観察、シリアル通信ケーブルを介したデバッグターミナル上での観察、MFDの印刷出力結果やファクス受信時動作の目視観察が行われている。

b.　実施テストの範囲

テストは開発者によって43項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのTSFIが十分にテストされたことが検証されている。深さ分析が実施され、TOE設計に記述されたすべてのTSFサブシステムのふるまいと相互作用が十分にテストされたことが検証されている。

c.　結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

7.4.2 評価者独立テスト

評価者は、確認のため開発者テストの一部をサンプリングし実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1）独立テスト環境

評価者が実施したテストの構成を図 7-2に示す。本構成はMFDに接続された外部電話機を除いて開発者テストと同様の構成である。
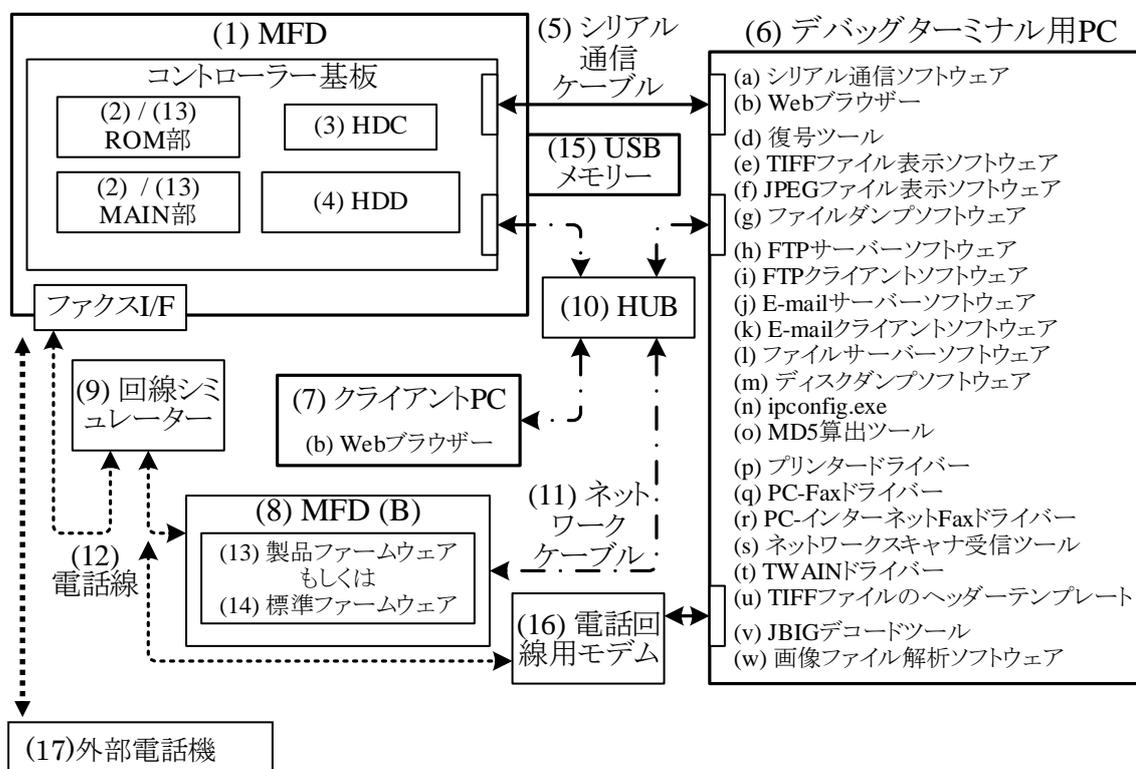
図 7-2　評価者テストの構成図

2）評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a.　独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

＜独立テストの観点＞

① 入力パラメタの網羅性の観点から開発者テストが不足していると判断されるTSFに関して、入力パラメタの種類、組み合わせを追加し、TSF毎にテストを実施する。

② 利用者操作のタイミング、組み合わせを追加し、TSFの振る舞いをより厳密に確認するためのテストを実施する。

③ クライアントPCとの接続方法に関して、開発者テストとは異なるインタフェースを使用しTSFの振る舞いを確認するためのテストを実施する。

④ TOEが提供する全てのインタフェースタイプ、及び全てのセキュリティ機能を網羅できるように考慮する。

b. 独立テスト概要

評価者が実施した独立テストの概要は以下のとおり。

＜独立テスト手法＞

開発者テストと同様のテスト手法が用いられた。

＜独立テストツール＞

開発者テストにおいて利用した表 7-2のツールを用いた。

＜独立テストの実施＞

独立テストの観点に基づき、独自テスト11件、サンプリングテスト13件のテストが実施された。実施された主なテスト内容と対応する独立テストの観点を表 7-3に示す。

表 7-3 実施した主な独立テスト

独立テストの観点	テスト概要
②、④	バックアップデータをリストアした場合でもセキュリティ機能が正常に動作する事を確認するためのテスト。
③、④	USB接続されたクライアントPCからのプリンタージョブ操作に関するテスト。
②、④	保存された親展ファイルのパスワード変更、ファイル消去のキャンセル処理、コピー作業中の割り込み処理等、複数のユーザー操作を追加した

	場合の上書き消去機能の正常動作を確認するためのテスト。
②、④	保存された親展ファイルの属性を運用中に変更された場合、及び複数の親展ファイルがロックされている状況でもセキュリティ機能が正常に動作する事を確認するためのテスト。
①、④	IPアドレス、MACアドレスの組み合わせを追加したネットワーク保護機能（フィルタ機能）のテスト。
①、④	外部電話機を接続した環境下でのファクスフロー制御機能のテスト。

c. 結果

実施したすべての評価者独立テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① telnet、ftp経由でTOEの保護資産及びOSに不正にアクセスされる可能性がある。

② 意図しないネットワークポートインタフェースが存在し、そこからTOEにアクセスできる可能性がある、もしくはオープンポートへの不正なデータ送信により保護資産が暴露される可能性がある。

③ 通常使用されることが想定されないインタフェースの使用、もしくは想定以外の使用方法でのインタフェースへのアクセスによりセキュリティ機能をバイパスされる可能性がある。

④ 必要以上の情報がインタフェースから出力され、秘密情報が暴露される可能性がある。

⑤ 想定外のユーザー操作、例外事象の発生タイミングによりセキュリティ機能がバイパスされる可能性がある。

⑥ 識別認証機能におけるパスワード処理に脆弱性が存在し、セキュリティ

機能がバイパスされる可能性がある。

⑦ SSLの実装に脆弱性が存在し、セキュリティ機能がバイパスされる可能性がある。

⑧ 想定外の設定値（制限範囲外の値、不正な値）が入力され、セキュリティ機能がバイパスされる可能性がある。

⑨ 複数台の複合機が連携して処理を実施する際に、TOEが未設置の複合機から保護資産が漏えいする可能性がある。

⑩ メモリー、及び内部基板に対する物理的な操作、及び想定外のアクセスにより、セキュリティ機能がバイパスされる可能性がある。

⑪ クライアントPCからのWeb経由でのアクセスにおいて脆弱性が存在し、セキュリティ機能がバイパスされる可能性がある。

b. 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストは評価者独立テストと同一のテスト構成で実施された（侵入テストで使用されるツールがインストールされたクライアントPCが追加されたのみである）。

侵入テストでは、表 7-2に示した開発者テストで使用したツールに加え、表 7-4に示したツールが使用された。

表 7-4 侵入テストで使用されたツール

ツール・ソフトウェア名称	概要・利用目的
FTP	ftp(ファイル転送プロトコル)クライアントソフト
netcat (1.11)	TCP,UDPパケットを読み書きするためのツール
nmap (6.46) zenmap (6.46)	ポートスキャンツール
telnet	telnet（リモートログインプロトコル）クライアントソフト
Wireshark (1.12.0(64-bit))	LAN上の通信をモニタ、解析するツール。

<脆弱性テストの実施>

潜在的な脆弱性の探索において識別された、懸念される脆弱性と対応する侵入テストの概要を表 7-5に示す。評価者は潜在的な脆弱性が悪用される可能性の有無を決定するため、21件の侵入テストを実施した。

表 7-5　侵入テスト概要

脆弱性	テスト概要
①	FTP、telnet経由でMFDに接続し、保護資産、システム関連情報に直接アクセスができないことを確認する。
②	ポートスキャンツールを使用し、意図しないネットワークポートが開いていないことを確認する。また、使用中のポートについても不正入力に対する脆弱性が存在しないことを確認する。
③	サービスマンインタフェースの不正使用、USBインタフェースへの機器接続からセキュリティ機能への侵害が発生しないことを確認する。
④	秘密情報の暴露に繋がる情報がTOEのインタフェースから出力されないことを確認する。
⑤	ガイダンスとは異なるユーザー操作、処理中のネットワーク遮断等が発生した場合でもセキュリティ機能のバイパスに繋がらないことを確認する。
⑥	不正なパスワード値や制限値以上の入力を行った場合でも、識別認証機能がバイパスされないことを確認する。
⑦	SSL接続の際、クライアントPC側の設定によって脆弱なプロトコルが選択されてしまうことがないことを確認する。
⑧	ネットワーク保護機能（フィルタ機能）の設定値に不正なアドレスを設定してもセキュリティ機能がバイパスされないことを確認する。
⑨	連結コピー実施時に、TOEが設置されないMFDから保護資産が漏えいしないことを確認する。
⑩	ROM、内部基板の差換え、抜き取り、不正アクセス等によりセキュリティ機能のバイパスに繋がる脆弱性が存在しないことを確認する。
⑪	Webブラウザー経由でのMFDへの接続時に指定するURLによりセキュリティ機能がバイパスされないことを確認する。

c.　結果

実施した評価者侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5 評価構成について

本評価では、「7.3.2 評価者独立テスト」及び図 7-2に示す構成において評価を行った。ネットワークはIPv4を使用している。TOEは、上記と構成要素が大きく異なる構成において、運用される場合はない。よって評価者は、上記評価構成が適切であると判断した。

7.6 評価結果

評価者は、評価報告書をもってTOEがCEMのワークユニットすべてを満たしていると判断した。

評価では以下について確認された。

- PP適合：なし
- セキュリティ機能要件： コモンクライテリア パート２適合
- セキュリティ保証要件： コモンクライテリア パート３適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- EAL3パッケージのすべての保証コンポーネント

評価の結果は、第2章で識別されたTOEについて、本章の評価された構成のみに適用される。

7.7 評価者コメント/勧告

消費者に喚起すべき評価者勧告は特にない。

8 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
② 評価報告書に示された評価者の評価判断の根拠が妥当であること。
③ 評価報告書に示された評価者の評価方法がCEMに適合していること。

8.1 認証結果

提出された評価報告書、及び関連する評価証拠資料を検証した結果、認証機関は、TOEがCCパート3のEAL3に対する保証要件を満たすものと判断する。

8.2 注意事項

TOEの利用者は、「4.2 使用環境構成」、及び「4.3 使用環境におけるTOE範囲」の記載内容を参照し、ネットワーク環境に関する運用上の要求事項が、実際のTOE運用環境において対応可能であるかどうかについて注意する必要がある。

9　附属書

特になし。

10　セキュリティターゲット

TOEのセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

MX-FR44 セキュリティターゲット バージョン 0.01　2014年2月19日
シャープ株式会社

11 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用されたTOEに関する略語を以下に示す。

DSK	データセキュリティキットMX-FR44 — MFDの別売オプション品。TOEのファームウェア部分を含む。
EEPROM	Electronically Erasable Programmable ROM — 不揮発性メモリーの一種で、低頻度であれば電気的に任意部分の書き換えを可能にしたROM。
HDC	Hard Disk Controller (ハードディスクコントローラー) — MFD内のHDCはTOEのハードウェア部分を含む。
HDD	Hard Disk Drive (ハード ディスク ドライブ)
HTTPS	HTTP over SSL — SSLにより保護されたHTTP。
IPP-SSL	IPP over SSL — SSLにより保護されたIPP。
MAC	Media Access Control (媒体アクセス制御) — 多数の通信機器が単一の通信媒体を共有できるよう、各機器を識別し、通信どうしが衝突しないよう調停する通信プロトコルの総称。
MFD	Multi Function Device — デジタル複合機。事務機であり、主としてコピー機能、プリンター機能、スキャナー機能及びファクス機能を有する。
MSD	Mass Storage Device — 大容量ストレージ装置。本STではMFD内のHDDを指す。

ROM	Read Only Memory — 読み出し専用メモリー。
USB	Universal Serial Bus — IT機器間を接続するシリアルバス標準の名称。

本報告書で使用された用語の定義を以下に示す。

IPアドレス	IPにおいて通信相手となる各機器を識別するための呼出符号。
MACアドレス	MACにおいて通信媒体上の各機器を識別するための呼出符号。
イメージデータ	本書では特に、MFDの各機能が扱う二次元画像のデジタルデータを指す。
インターネットFax	インターネット経由でファクシミリ情報を送受信する機能。標準仕様に従い、ファクシミリデータをメール添付ファイルとして送受信する。
揮発性メモリー	電源を切れば記憶内容が消失する記憶装置。
コントローラー基板	MFD全体を制御する基板。TOEのファームウェアを実行するためのCPU、揮発性メモリー、HDC、HDD 等を有する。
コントローラーファームウェア	MFDのコントローラー基板を制御するファームウェア。
サブネットワーク	内部ネットワークのうち、ルータで区切られた範囲。
ジョブ	MFDのコピー、プリンター、スキャナー、ファクス送受信及びPC-Faxの各機能において、その機能の開始から終了までの流れ、シーケンス。また、機能動作の指示についてもジョブと呼ぶ場合がある。
親展ファイル	利用者がファイリング保存したデータのうち､他人に無断で再利用されないよう、パスワード（親展ファイルパスワード）によって保護されたもの。
スプール	入出力効率のため、ジョブのイメージデータを一時的にMSDに保存すること。
操作パネル	MFDの正面にあるUI用ユニット。スタートキー、数字キー、機能キー及びタッチ操作式の液晶ディスプレイを含む。
ドキュメントファイリング	MFDが取り扱うイメージデータを、利用者が後で再操作できるようMFD内のHDDに保存する機能。本書では、ファイリングと

	も呼ぶ。
標準ファームウェア	TOE設置前のMFDに搭載されているコントローラーファームウェア。TOEはコントローラーファームウェアを含んでおり、TOE設置時に標準ファームウェアはTOEのコントローラーファームウェアに置き換えられる。
不揮発性メモリー	電源を切っても記憶内容を保持することができる記憶装置。
プリンター機能	外部より受信したデータを印刷する機能。
ホールド	プリンタードライバーからのジョブを、ファイリング保存すること。
連結印刷	大量の印刷部数を2台のMFDで折半することにより倍速でこなす機能。
連結コピー	MFDのコピー機能における連結印刷のこと。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程　平成26年3月
独立行政法人情報処理推進機構　CCS-01

[2] ITセキュリティ認証等に関する要求事項　平成26年4月
独立行政法人情報処理推進機構　CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項　平成25年4月
独立行政法人情報処理推進機構　CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 4,September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン3.1 改訂第4版 2012年9月, CCMB-2012-09-001,(平成24年11月翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-002,(平成24年11月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-003,(平成24年11月翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第4版, 2012年9月, CCMB-2012-09-004 (平成24年11月翻訳第1.0版)

[12] MX-FR44 セキュリティターゲット バージョン 0.01　2014年2月19日
シャープ株式会社

[13] MX-FR44 評価報告書 第4.3版 2014年11月25日
一般社団法人　ITセキュリティセンター　評価部